

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-12. (Cancelled)

13. (Currently Amended) A pseudo random number generator comprising:
a cipher unit to generate a sequence of ciphering bits to cipher a stream of data
including at least video data; and
a state machine coupled to the cipher unit to also use the ciphering unit to
generate a plurality of pseudo random numbers based on selected ones of said cipher bits
wherein the state machine is equipped to transition to a continuous clocking state that
includes, upon power on or reset, causing the cipher unit to be continuously clocked to
introduce entropy into the cipher unit.

14. (Original) The pseudo random generator of claim 13, wherein the state
machine operates in a selected one of a continuous clocking state, a first cipher bit taking
state, an output state, a second cipher bit taking state, and an authenticated state, wherein
the state machine causes the cipher unit to be continuously clocked while in said
continuous clocking state to introduce entropy in said cipher unit, causes first and second
plurality of said cipher bits to be taken and stored, in said first and second cipher bit
taking states respectively, causes the stored first/second cipher bits to be output as

first/second random numbers, causes the cipher bits of the cipher unit to be used to cipher said stream of data during said authenticated state.

15. (Previously Presented) The pseudo random generator of claim 14, wherein the state machine is equipped to transition from said continuous clocking state to said first cipher bit taking state, in response to a subsequent request after n clocks for said first pseudo random number, where n is an integer, and to transition from said first cipher bit taking state to said output state, upon storing the first output cipher bits.

16. (Previously Presented) The pseudo random generator of claim 14, wherein the state machine is equipped to transition from said output state to a selected one of the continuously clocking state, the second cipher bit taking state, and the authenticated state depending on whether upon provision of the first pseudo random number, an indication of an unsuccessful authentication using the first pseudo random number, another request for a second pseudo random number, or an indication of a successful authentication using the first pseudo random number is received.

17. (Previously Presented) The pseudo random generator of claim 14, wherein the state machine is equipped to transition from said second cipher bit taking state to said output state upon taking the second plurality of output cipher bits of the cipher unit and storing the second output cipher bits.

18. (Previously Presented) The pseudo random number generator of claim 14, wherein the state machine is further equipped to transition from said authenticated state to said second cipher bit taking state upon receiving another request for a third pseudo random number, and to said continuously clocking state upon receiving a selected one of an unauthenticated notification and a detachment notification.